PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-273705
(43)Date of publication of application : 05.10.2001

(51)Int.Cl. G11B 19/04
G11B 7/004
G11B 7/007
G11B 19/02
G11B 20/10

(21)Application number : 2000-028053
(22)Date of filing : 04.02.2000

(71)Applicant : SONY CORP
(72)Inventor : IIDA MICHIHIKO

(30)Priority
Priority number : 2000009381 Priority date : 18.01.2000 Priority country : JP

(54) RECORDING MEDIUM ITS IDENTIFYING METHOD AND ITS RECORDING AND REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent altering and forging of important file data such as approval and settlement of accounts of a programmable recording medium.
SOLUTION: In the recording medium its identification method and the recording and reproducing device of the recording mediumrandom analog waveform signals are recorded into a programmable recording medium. The signals are registered as identification datai.e.fingerprint data. The data are transferred to a host computer and stored as a fingerprint intrinsic to a recording medium. During a reprogramming to the mediumthe fingerprint data stored in the host computer and the fingerprint data of the recording medium are compared and a writing approval is given when the comparison result falls within a prescribed comparison range value.

CLAIMS

[Claim(s)]
[Claim 1]A recording medium being a recording medium in which re-writing is possiblehaving recorded a random waveform pattern in a prescribed data record

section of the above-mentioned recording mediumand making with identification data of this recording medium.
[Claim 2]The recording medium according to claim 1wherein said random waveform pattern is the identification data which shook and acquired a laser power value within a prescribed range value with random data generated by a random number generation means.
[Claim 3]The recording medium according to claim 1wherein said random waveform pattern is the identification data which shook and acquired a focus bias value in a prescribed range with random data generated by a random number generation means.
[Claim 4]A record step which records a random waveform pattern in a prescribed data record section of a recording medium in which re-writing is possibleA memory step which incorporates a random waveform pattern recorded at the above-mentioned record stepis sent out to a host computerand is memorized as identification data to a memory measure in this host computerA random waveform pattern recorded at the above-mentioned record step at the time of writing to the above-mentioned recording medium is readsending out to the above-mentioned host computer as digital data -- this host computer -- this -- it being sent out and digital data as compared with identification data within the above-mentioned memory measureAn identifying method of a comparison step which will permit writing to this recording medium if this comparison data is a predetermined value within the limitsand a recording medium changing more.
[Claim 5]A recording and reproducing device of a recording medium which is provided with the following and characterized by accomplishing the above-mentioned host computer so that re-write-in permission or disapproval data may be sent out.
A recording device which records a random waveform pattern in a predetermined data writing field of a recording medium in which re-writing is possible.
A reproduction means which reproduces a random waveform pattern recorded by the above-mentioned recording deviceand is sent out to a host computer.
the above sent out to the above-mentioned host computer -- a random waveform pattern being memorized to this host computerand it being considered as identification data of a recording mediumandA comparison means [host computer / this / this identification data / waveform pattern / which the above-mentioned reproduction means sent out to this host computer at the time of re-writing of a recording medium / random].

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]With respect to a recording medium in which re-writing is

possiblean identifying method for the sameand its recording and reproducing deviceespeciallythis invention is used for the recorder of the recording medium in which re-writing is possibleand relates to a suitable recording mediuman identifying method for the sameand its record re-device.
[0002]
[Description of the Prior Art]From the formersince the copy from various recording media or alteration of computer softwareimage softwarevoice softwareetc. is comparatively easythe prevention measure for preventing these illegal copies and an alteration is taken. These prevention measures record a unique code on the recording medium itself logically or physically fundamentallyalthough many methods are proposedand it is being identified by reading this whether it is an inaccurate or regular recording medium.
[0003]For examplein JPH7-176080Athe recording medium which attained differentiation with the recording medium which was formed by regenerated light by having made into security information the pattern code which can be read at the time of recording-medium creationand was physically copied in the data recording regions of a recording medium and outside the record section is indicated.
[0004]The recording medium which recorded security information logically in the same format to which the usual thing and distinction are not attached using rupture of a hour entry in the buffer space in the inner circumference in a recording-medium management domainand its check device are indicated by JPH8-153342A.
[0005]
[Problem(s) to be Solved by the Invention]RecentlyCD-RW (Compact Disc Rewritable)DVD-RAM (Digital Versatile Disc-RAM)The recording medium in which re-writingsuch as MO (Magnet Optical disc) and magnetic tapeis possibleOr CD-R (Compact Disc Recordable)Recording mediasuch as WORM (Write Once Read Many opticaldisc: write once optical disk)such as DVD-R (Digital Versatile Disc Recordable)have appeared on the market widely. The recording medium which prevented the copy and the alteration by the above-mentioned security information has many which have managed security information with digital data only for reproduction.
[0006]In the recording medium in which above-mentioned re-writing is possibleor a recording medium like WORMwhen recording and electronic-file-izing the important matter which needs recognitionsettlement of accountsattestationetc.an unjust alteration or forgery needs to be made not to be made recordable to the recording medium itselfbut. When putting the identification information as security information into a recording medium physically as mentioned abovemany equipment is needed and the compatibility between marketed recording mediaetc. pose a problem.
[0007]When the identification information as security information was logically put into a recording medium and security information was managed with digital data on the other handsecurity information was decoded theoretically and there was a

problem whose alteration and forgery are attained.
[0008]This invention was made in order to cancel above-stated SUBJECTand it tends to provide a recording medium which recorded the security information which identification information cannot decode easilyan identifying method for the sameand its recording and reproducing device.
[0009]
[Means for Solving the Problem]A recording medium of the 1st this invention is a recording medium in which re-writing is possiblerecords a random waveform pattern in a prescribed data record section of this recording mediumand forms it with identification data of a recording medium.
[0010]A recording medium of the 2nd this invention records identification data which shook and acquired a laser power value within a prescribed range value with random data made to generate the random waveform pattern by a random number generation means.
[0011]A recording medium of the 3rd this invention records identification data which shook and acquired a focus bias value within a prescribed range value with random data made to generate said random waveform pattern by a random number generation means.
[0012]A record step which records a random waveform pattern in a prescribed data record section of a recording medium which the identifying method of a recording medium of this invention can re-write inIncorporate a random waveform pattern recorded at this record stepand it sends out to a host computerA memory step memorized as identification data to a memory measure in a host computerA random waveform pattern recorded at a record step at the time of writing to a recording medium is readIt sends out to a host computer as digital dataand a host computer comprises a comparison step which permits writing to a recording mediumif this comparison data is a predetermined value within the limits about this sending-out ****** digital data as compared with identification data within a memory measure.
[0013]A recording device which records a random waveform pattern in predetermined data recording regions of a recording medium which the recording and reproducing device of a recording medium of this invention can re-write inA reproduction means which reproduces a random waveform pattern recorded by this recording deviceand is sent out to a host computerA host computer memorizes a random waveform pattern sent out to a host computerand uses it as identification data of a recording mediumIt has a comparison means [host computer / identification data / waveform pattern / which a reproduction means sent out to a host computer at the time of re-writing of a recording medium / random]and a host computer is accomplished so that re-write-in permission or disapproval data may be sent out.
[0014]Since an analog random waveform is recorded as identification data according to the above-mentioned 1st thru/or the 3rd recording mediumpowerful protection is attained with identification data which is hard to decode as compared with a case where identification data which is security information in digital one is

processed.
[0015]According to the identifying method of an above-mentioned recording mediuman identifying method which cannot alter or forge easily an electronic file which needs recognitionsettlement of accountsetc. is acquired simply.
[0016]If it is a recording and reproducing device which has an optical pickup in which record reproduction is possible for data of a recording medium according to the recording and reproducing device of an above-mentioned recording mediuma recording and reproducing device which can record identification data will be obtained simplywithout forming a special device.
[0017]
[Embodiment of the Invention]Hereafterdrawing 1 thru/or drawing 8 explain the example of 1 gestalt of this invention.
[0018]Drawing 1 shows the distribution diagram of the recording and reproducing device of this inventionand explains the recording and reproducing device of CD-R which is a write once optical disk as a recording medium.
[0019]In drawing 1the recording and reproducing device 28 is connected to the host computer (it is hereafter described as H.CPU) 26 via a busand H.CPU26 has the memory measures 27such as a hard disk drive (HDD).
[0020]Having the recording medium (it is described as CD-R below) 1 in the recording and reproducing device 28this CD-R1 formed the pregroove on the synthetic resin base 1aand it formed the reflecting layers 1csuch as goldon the recording layers 1bsuch as coloring matter of a cyanogen systemand has covered this reflecting layer 1c top with 1 d of protective layers.
[0021]CD-R1 is laid on the turntable 2it rotates with the spindle motor 3and drive controlling of the spindle motor 3 is carried out via the servo circuit 20 and the spindle drive circuit 23.
[0022]By the slide motor 4the optical pickup 5 and the high power laser 6 are made as it is movable to the spoke direction of CD-R1. The slide motor 4 carries out slide - controlling of the optical pickup 5 or the high power laser 6 via the servo circuit 20 and the slide drive circuit 22.
[0023]A writing control signal is supplied to the laser drive circuit 8 through RF amplifier 9 from CPU17 at the time of the re-writing to CD-Rand the high power laser 6 carries out drive controlling of the high power laser 6and the power of the high power laser 6 is monitored by the laser power monitor 7.
[0024]As for the optical pickup 5drive controlling of the control of a focus and the biaxial direction of tracking is carried out via the servo circuit 20 and the biaxial actuator drive circuit 21.
[0025]The RF signal from RF amplifier 9 and the control signal from CPU17 are supplied to the servo circuit 20. The catoptric light taken up by the optical pickup 5 is changed into an electrical signaloutputs an RF signal via RF amplifier 9and is supplied to the RF processing circuit 10.
[0026]An RF signal carries out an EFM (8 -14 abnormal conditions) recovery after synchronous detection in the synchronous detection circuit 12 via the PLL (Phase Locked Loop) circuit 11 in the RF processing circuit 10By the encoder / decoder

15it encodes and decodesand the acquired EFM signal is supplied to H.CPU26 of the exterior via I/F(interface) 16and is stored in the memory measure 26 of H.CPU26.
[0027]The push pull signal of the RF signal acquired from RF amplifier 9 is supplied to the ATIP (Absolute Time In Pregrove) decoder 13 in the RF signal processing circuit 10aargh -- the pregroove by which the bull was carried out -- aarghbull processing is performed and the synchronous interrupt user data and the address decode result of ATIP are given to CPU17.
[0028]Re-write data is given from H-CPU26 and EFM data drives the power laser 6 through RF amplifier 9 and the laser drive circuit 8 via I/F16and the encoder/decoder 15.
[0029]CPU17 has ADC (analog-digital converter)18 and DAC (digital-to-analog converter)19The data which digitized the RF signal via ADC18 from RF amplifier 9 is given to CPU17The analog pattern waveform which serves as identification data (fingerprint peculiar to a recording medium which spaces through CD-R and is written in as art) as security information from CPU17 via DAC19 is supplied.
[0030]In an above-mentioned recording and reproducing devicedrawing 2 and drawing 3 explain the composition which writes identification data (it is described as fingerprint data below) in CD-R1. Although identical codes are given to a corresponding point with drawing 1 by drawing 2 and drawing 3 and duplication explanation is omitteddrawing 2 is a case where laser power control is performedand drawing 3 shows the distribution diagram in the case of also performing focus bias control.
[0031]In drawing 2although it may be included in CPU17the random number generation means 24 is prepared and random data is generated by this random number generation means 24. Supply this random data to DAC19and in order to shake by the desired value of the laser power of the high power laser 6 by the random signal which carried out analogue conversion by DAC19the noninverting terminal of RF amplifier 9 is suppliedHe connects a laser power monitor to an inversion terminaland is trying to drive the high power laser 6 via the laser drive circuit 8.
[0032]In order to shake the amount of focus bias (offset) of the optical pickup 5 by random data in drawing 3 and to write fingerprint data in the recording layer 1bThe random signal obtained from DAC19 is supplied to the inversion terminal of the summing amplifier 25The RF signal acquired via the optical pickup 5 and RF amplifier 9 is supplied to the noninverting terminal of the summing amplifier 25a summing amplifier output is supplied to the optical pickup 5 via the servo circuit 20 and the focus driving circuit 21aand the writing of a fingerprint is performedshaking focus bias.
[0033]The flow chart of drawing 4 thru/or drawing 6 and the wave form chart of drawing 7 and drawing 8 explain operation with the distribution diagram explained by above-mentioned drawing 1 and drawing 2.
[0034]Drawing 4 shows the flow chart at the time of the writing of the fingerprint data of CD-R1. In drawing 4the prescribed position of CD-R1 is accessed by 1st

step S_1.
[0035]In 2nd step S_2a random numerical value is generated by the random number generation means 24.
[0036]In 3rd step S_3laser power is controlled by the random numerical value acquired by 2nd step S_2 like drawing 2and the fingerprint data which is identification data is written in the prescribed position of CD-R1 in analog.
[0037]In 4th step S_4writing is stopped at the time of the write end of the predetermined regenerative waveform 29 as shown in drawing 7and it results in an end.
[0038]Drawing 5 shows the flow chart at the time of registration of the fingerprint data of H-CPU26and accesses the optical pickup 5 in 1st step ST_1 at the predetermined specified position of CD-R1.
[0039]In 2nd step ST_2read-out of the fingerprint data written in CD-R1 is started.
[0040]In 3rd step $ST_3$the fingerprint data recorded on CD-R1 is changed into digital data via DAC19and it transmits to H-CPU26.
[0041]By 3rd step ST_3as fingerprint data. the case where the regenerative waveform 29 like drawing 7 is obtained -- Time $t_1t_2t_3$and t_4 .... t_i .... the digital conversion value by ADC18 of t_n -- respectively -- $A_1A_2A_3$and A_4 .... A_i .... it being considered as $A_n$and the whole data row being set to Wvdtandlt is considered as data set value W_i= (t_iA_n) in digital conversion value A_i at the time of time t_i.
[0042]The necessity of normalizing since it differs by reproduction conditionssuch as a gaindispersion of the drive characteristicaging of CD-R1etc. produces above-mentioned digital conversion value A_i.
[0043]For examplethe repetition regenerative waveform 29 shown in drawing 7 of mT=4T. If the value after each ADC at the time of being $V_1V_2V_3$and V_4 is set with $pk_1pk_2pk_3$and pk_4 as the level of a peak two-piece (Peak to Peak) when it writes in CD-R1 shows drawing 8Average value pk-ave of this peak two-piece value pk_1 - pk_4 is pk-ave=(pk_1+pk_2+pk_3+pk_4) /4... (1)
It becomes.
[0044]A_i is normalized with the regeneration level of 4T here (Normalize). That isit will be B_i=A_i/pk-ave if normalized peak value is made into B_i.... (2)
It can come out and express.
[0045]Nextin 4th step $ST_4$the normalized above-mentioned regenerative waveform 29 is stored in the nonvolatile memory measure 27 which H-CPU26 has with the management number of CD-R1and registration is ended for this as the security information of CD-R1i.e.fingerprint data.
[0046]Although the random patterni.e.fingerprint datarecorded on CD-R1 was incorporated as an analog-spectrum form by ADC and the waveform was stored in H-CPU26 via ADC with above-mentioned compositionIt may be made to store in H-CPU26 the fingerprint data which binary-ized the random pattern of CD-R1 with the high-speed sample rate quicker than usual.
[0047]Nextdrawing 6 explains the flow chart of the write-in permission to CD-R1and disapproval processing. With the recording and reproducing device 28this flow chart reads the fingerprint data recorded on CD-R1compares it with the

fingerprint data stored in H-CPU26and accesses the optical pickup 5 by 1st step STP_1 in a prescribed position.
[0048]In 2nd step $STP_2$the lead of the fingerprint data written in CD-R1 is started.
[0049]Although all the data row Wvdt(s) of the fingerprint data shown by drawing 7 with the disk management number of CD-R1 are registered into H-CPU26this is set to Wvdto and peak value B_i normalized by above-mentioned (2) formulas is made into R_i. Namely$R_i=B_i$ ($1 <=i<=S$) ... (3)
S is the number of W_i here.
[0050]In 3rd step $STP_3$the recording and reproducing device 28 reads in analog the fingerprint data recorded on CD-R1 read via the optical pickup 5and transmits all the data row Wvdt(s) which carried out digital conversion via ADC18 to the H-CPU26 side.
[0051]In 4th step STP_4H-CPU26 takes out fingerprint data $Wvdt_0$ (set of R_i) of the disk corresponding to the disk management number of CD-R1 from the memory measure 27.
[0052]5th step STP_5 compares fingerprint data Wvdt (set of B_i) of all the data rows of CD-R1 transmitted by 3rd step STP_3.
[0053]These comparison operations are $R_i+Wdu>B_i>R_i-Wdl$... (4)
Hereit is an acceptable value of the Wdu: upper part. It is an acceptable value of the Wdl: bottom. It becomes.
[0054]When F is made into the total number of B_i ($1 <=i<=S$) which fills (4) types noweta=F/S is definedand the following conditions are considered at this time.
Eta>C ... (5)
C is an allowable ratiofor exampleis chosen to 70 percent - about 90 percent here.
[0055]It is judged whether it was satisfied with 6th step STP_6 of (5) types. That isH-CPU26 judges whether comparison data fulfilled the predetermined allowable ratio rateand if (5) types are not filledthe instructions which progress to 7th step STP_7 and forbid the writing of CD-R1 are transmitted to a recording and reproducing device.
[0056]On the other handin being satisfied with 6th step STP_6 of (5) typesit accomplishes so that it may progress to 8th step STP_8 and the write-in permission command of CD-R1 may be transmitted to a recording and reproducing device.
[0057]This invention is constituted like the above statementand since it operatesan alteration and the identifying method which cannot be forged can be illegally acquired for important electronic filessuch as the recording medium and recording and reproducing device which cannot be forgedand settlement of accountswith easy compositionSince the analog waveform was used as identification data (fingerprint data)the system in which powerful protection is possible is obtained also to electronic authentication.
[0058]
[Effect of the Invention]Since the analog random waveform is recorded as identification data according to the recording medium of this inventionpowerful protection is attained with the identification data which is hard to decode as

compared with the case where the identification data which is security information in digital one is processed.

[0059]According to the identifying method of the recording medium of this inventionthe identifying method which cannot alter or forge easily the electronic file which needs recognitionsettlement of accountsetc. is acquired simply.

[0060]If it is a recording and reproducing device which has an optical pickup in which record reproduction is possible for the data of a recording medium according to the recording and reproducing device of the recording medium of this inventionthe recording and reproducing device which can record identification data will be obtained simplywithout forming a special device.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a distribution diagram of the recording and reproducing device of this invention.

[Drawing 2]It is a distribution diagram of the laser power control part of this invention.

[Drawing 3]It is a distribution diagram of the focus bias control section of this invention.

[Drawing 4]It is a flow chart of the writing of the identification data to the recording medium of this invention.

[Drawing 5]It is a flow chart at the time of registration of the identification data to the host computer of this invention.

[Drawing 6]It is a flow chart of the write-in permission to the recording medium of this inventionand disapproval processing.

[Drawing 7]It is a sample timing wave form chart of the regenerative waveform for explanation of this invention of operationand ADC.

[Drawing 8]It is a calibration regenerative waveform figure of the explanatory view of this invention of operation.

[Description of Notations]

1 [.... A laser drive circuit9 / .... An RF amplifier10 / .... RF processing circuit17 / .... CPU24 / .... A random number generation means25 / .... A summing amplifier26 / .... H-CPU27 / .... Memory measure] .... A recording medium (CD-R)5 .... An optical pickup6 .... Power laser8

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－273705
（P2001－273705A）
(43)公開日　平成13年10月５日(2001.10.5)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ１１Ｂ	19/04	５０１	Ｇ１１Ｂ 19/04	５０１Ｈ	５Ｄ０４４
	7/004		7/004	Ｃ	５Ｄ０６６
	7/007		7/007		５Ｄ０９０
	19/02	５０１	19/02	５０１Ｊ	
	20/10		20/10	Ｈ	

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

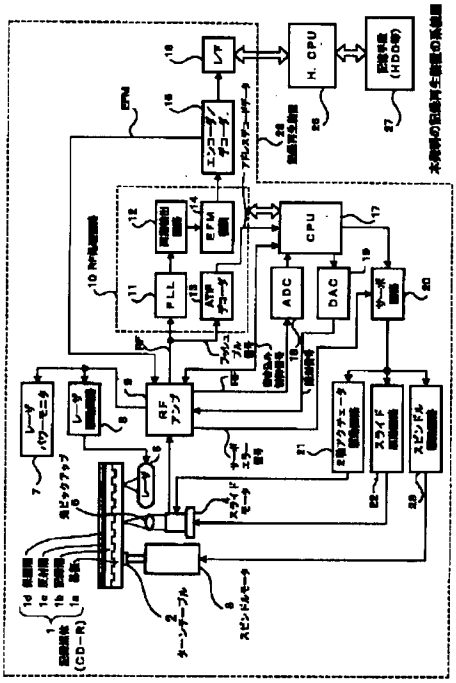
(21)出願番号　特願2000－28053(P2000－28053)
(22)出願日　平成12年２月４日(2000.2.4)
(31)優先権主張番号　特願2000－9381(P2000－9381)
(32)優先日　平成12年１月18日(2000.1.18)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　飯田　道彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100080883
弁理士　松隈　秀盛

Ｆターム(参考)　5D044 BC06 CC04 DE49 DE50 DE52
GK17 HL08
5D066 DA04 DA12 DA16
5D090 AA01 BB04 CC01 DD03 DD05
FF09 FF31 FF41 FF49 GG32
GG33

(54)【発明の名称】　記録媒体及びその識別方法並びにその記録再生装置

(57)【要約】
【課題】　書き込み可能な記録媒体への承認、決済等の重要ファイルデータの改竄、偽造を強力に防止する。
【解決手段】　書き込み可能な記録媒体へランダムなアナログ的な波形信号を記録し、識別データ、即ち指紋データとして登録し、この指紋データをホストコンピュータに転送して記録媒体固有の指紋として格納して置き、記録媒体への再書き込み時にホストコンピュータに格納した指紋データと記録媒体の指紋データを比較し、所定比較範囲値内に入ったときのみ書き込み許可を与える様にした記録媒体及びその識別方法並びに記録媒体の記録再生装置を提供する。



【特許請求の範囲】
【請求項１】　再書き込み可能な記録媒体であって、
上記記録媒体の所定データ記録領域内にランダムな波形パターンを記録し、該記録媒体の識別データとなしたことを特徴とする記録媒体。
【請求項２】　前記ランダムな波形パターンは乱数発生手段で発生させたランダムデータによってレーザパワー値を所定範囲値内で振って得た識別データであることを特徴とする請求項１記載の記録媒体。
【請求項３】　前記ランダムな波形パターンは乱数発生手段で発生させたランダムデータによってフォーカスバイアス値を所定範囲内で振って得た識別データであることを特徴とする請求項１記載の記録媒体。
【請求項４】　再書き込み可能な記録媒体の所定データ記録領域内にランダムな波形パターンを記録する記録ステップと、
上記記録ステップで記録したランダムな波形パターンを取り込んでホストコンピュータに送出して該ホストコンピュータ内の記憶手段に識別データとして記憶する記憶ステップと、
上記記録媒体への書き込み時に上記記録ステップで記録したランダムな波形パターンを読み出し、デジタルデータとして上記ホストコンピュータに送出し、該ホストコンピュータはこの送出されデジタルデータを上記記憶手段内の識別データと比較し、この比較データが所定の範囲内の値であれば該記録媒体への書き込みを許可する比較ステップと、
より成ることを特徴とする記録媒体の識別方法。
【請求項５】　再書き込み可能な記録媒体の所定のデータ書き込み領域内にランダムな波形パターンを記録する記録手段と、
上記記録手段で記録したランダムな波形パターンを再生し、ホストコンピュータに送出する再生手段と、
上記ホストコンピュータに送出した上記ランダムな波形パターンを該ホストコンピュータに記憶して記録媒体の識別データとし、記録媒体の再書き込み時に上記再生手段が該ホストコンピュータに送出したランダムな波形パターンを該ホストコンピュータは該識別データと比較する比較手段とを有し、
上記ホストコンピュータは再書き込み許可又は不許可データを送出するように成したことを特徴とする記録媒体の記録再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は再書き込み可能な記録媒体及びその識別方法並びにその記録再生装置に係わり、特に、再書き込み可能な記録媒体の記録装置に用いて好適な記録媒体及びその識別方法並びにその記録再装置に関する。
【０００２】
【従来の技術】従来からコンピュータソフト、映像ソフト、音声ソフト等の各種記録媒体からのコピー或は改竄は比較的容易であるため、これら不正コピーや改竄を防止するための防止措置がとられている。これら防止措置は多くの方法が提案されているが、基本的には記録媒体自体に特異なコードを論理的或は物理的に記録し、これを読み取ることで不正或は正規の記録媒体であるか等の識別を行なっている。
【０００３】例えば、特開平７－１７６０８０号公報では物理的に記録媒体のデータ記録領域内或は記録領域外に再生光により読み取り可能なパターンコードをセキュリティ情報として記録媒体作成時に形成し、コピーした記録媒体との差別化を図った記録媒体が開示されている。
【０００４】又、特開平８－１５３３４２号公報には記録媒体管理領域中の内周にあるバッファ領域内に通常のものと見分けの付かない同一フォーマットで、時間情報の断絶を利用してセキュリティ情報を論理的に記録した記録媒体及びそのチェック装置が開示されている。
【０００５】
【発明が解決しようとする課題】近時、ＣＤ－ＲＷ（Compact Disc Rewritable）、ＤＶＤ－ＲＡＭ（Digital Versatile Disc-RAM）、ＭＯ（Magnet Optical disc）、磁気テープ等の再書き込み可能な記録媒体、或はＣＤ－Ｒ（Compact Disc Recordable）、ＤＶＤ－Ｒ（Digital Versatile Disc Recordable）等のＷＯＲＭ（Write Once Read Many opticaldisc ：追記型光ディスク）等の記録媒体が広く出回っている。上記したセキュリティ情報でコピーや改竄を防止する様にした記録媒体は再生専用でデジタルデータでセキュリティ情報を管理しているものが多い。
【０００６】上述の再書き込み可能な記録媒体或はＷＯＲＭの様な記録媒体では例えば、承認、決済、認証等を必要とする重要な事項を記録して電子ファイル化する場合に記録媒体自身に記録が可能であり、且つ不正な改竄或は偽造ができないようにする必要があるが、上述のように物理的にセキュリティ情報としての識別情報を記録媒体に入れる場合は多くの設備を必要とし市販済の記録媒体との間での互換性等も問題となる。
【０００７】一方、論理的にセキュリティ情報としての識別情報を記録媒体に入れる場合にデジタルデータでセキュリティ情報の管理を行なう場合は原理的にはセキュリティ情報が解読され改竄や偽造が可能となる問題があった。
【０００８】本発明は叙上の課題を解消するためになされたもので、識別情報が解読しにくいセキュリティ情報を記録した記録媒体及びその識別方法並びにその記録再生装置を提供しようとするものである。
【０００９】
【課題を解決するための手段】第１の本発明の記録媒体

は再書き込み可能な記録媒体であって、この記録媒体の所定データ記録領域内にランダムな波形パターンを記録し、記録媒体の識別データとなしたものである。

【００１０】第２の本発明の記録媒体は前記したランダムな波形パターンを乱数発生手段で発生させたランダムデータによってレーザパワー値を所定範囲値内で振って得た識別データを記録したものである。

【００１１】第３の本発明の記録媒体は前記ランダムな波形パターンを乱数発生手段で発生させたランダムデータによってフォーカスバイアス値を所定範囲値内で振って得た識別データを記録したものである。

【００１２】本発明の記録媒体の識別方法は再書き込み可能な記録媒体の所定データ記録領域内にランダムな波形パターンを記録する記録ステップと、この記録ステップで記録したランダムな波形パターンを取り込んでホストコンピュータに送出して、ホストコンピュータ内の記憶手段に識別データとして記憶する記憶ステップと、記録媒体への書き込み時に記録ステップで記録したランダムな波形パターンを読み出し、デジタルデータとしてホストコンピュータに送出し、ホストコンピュータはこの送出ささたデジタルデータを記憶手段内の識別データと比較し、この比較データが所定の範囲内の値であれば記録媒体への書き込みを許可する比較ステップとより成るものである。

【００１３】本発明の記録媒体の記録再生装置は再書き込み可能な記録媒体の所定のデータ記録領域内にランダムな波形パターンを記録する記録手段と、この記録手段で記録したランダムな波形パターンを再生し、ホストコンピュータに送出する再生手段と、ホストコンピュータに送出したランダムな波形パターンをホストコンピュータは記憶して記録媒体の識別データとし、記録媒体の再書き込み時に再生手段がホストコンピュータに送出したランダムな波形パターンをホストコンピュータは識別データと比較する比較手段とを有し、ホストコンピュータは再書き込み許可又は不許可データを送出するように成したものである。

【００１４】上述の第１乃至第３の記録媒体によればアナログ的なランダム波形を識別データとして記録しているためデジタル的にセキュリティ情報である識別データを処理する場合に比較して解読し難い識別データによって強力なプロテクトが可能となる。

【００１５】又、上述の記録媒体の識別方法によれば承認、決済等を必要とする電子ファイルを容易に改竄或は偽造できない識別方法が簡単に得られる。

【００１６】更に、上述の記録媒体の記録再生装置によれば記録媒体のデータを記録再生可能な光ピックアップを有する記録再生装置であれば、特別の装置を設けずに簡単に識別データを記録可能な記録再生装置が得られる。

【００１７】

【発明の実施の形態】以下、本発明の１形態例を図１乃至図８によって説明する。

【００１８】図１は本発明の記録再生装置の系統図を示すものであり、記録媒体として追記型光ディスクであるＣＤ－Ｒの記録再生装置について説明する。

【００１９】図１に於いて、記録再生装置２８はホストコンピュータ（以下、Ｈ．ＣＰＵと記す）２６にバスを介して接続され、Ｈ．ＣＰＵ２６はハードディスクドライブ（ＨＤＤ）等の記憶手段２７を有している。

【００２０】記録再生装置２８内には記録媒体（以下ＣＤ－Ｒと記す）１を有し、このＣＤ－Ｒ１は合成樹脂基板１ａ上にプリグルーブを形成すると共にシアン系の色素等の記録層１ｂ上に金等の反射層１ｃを形成し、この反射層１ｃ上を保護層１ｄによって被覆している。

【００２１】ＣＤ－Ｒ１はターンテーブル２上に載置され、スピンドルモータ３で回転され、スピンドルモータ３はサーボ回路２０及びスピンドル駆動回路２３を介して駆動制御される。

【００２２】光ピックアップ５とハイパワーレーザ６はスライドモータ４によりＣＤ－Ｒ１の輻方向に移動可能となされている。スライドモータ４はサーボ回路２０とスライド駆動回路２２を介して光ピックアップ５やハイパワーレーザ６をスライド制御する。

【００２３】ハイパワーレーザ６はＣＤ－Ｒへの再書き込み時にＣＰＵ１７から書き込み制御信号がＲＦアンプ９を経て、レーザ駆動回路８に供給され、ハイパワーレーザ６を駆動制御すると共にレーザパワーモニタ７でハイパワーレーザ６のパワーがモニタされる。

【００２４】光ピックアップ５はフォーカス及びトラッキングの２軸方向の制御がサーボ回路２０と２軸アクチェータ駆動回路２１を介して駆動制御される。

【００２５】サーボ回路２０にはＲＦアンプ９からのＲＦ信号とＣＰＵ１７からの制御信号が供給されている。光ピックアップ５でピックアップされた反射光は電気信号に変換されＲＦアンプ９を介してＲＦ信号を出力し、ＲＦ処理回路１０に供給される。

【００２６】ＲＦ信号はＲＦ処理回路１０内のＰＬＬ(Phase Locked Loop)回路１１を介して同期検波回路１２で同期検波後にＥＦＭ（８－１４変調）復調し、エンコーダ／デコーダ１５でエンコード及びデコードし、得られたＥＦＭ信号はＩ／Ｆ（インタフェース）１６を介して外部のＨ．ＣＰＵ２６に供給され、Ｈ．ＣＰＵ２６の記憶手段２６に格納される。

【００２７】ＲＦアンプ９から得たＲＦ信号のプッシュプル信号はＲＦ信号処理回路１０内のＡＴＩＰ(Absolute Time In Pregrove)デコーダ１３に供給され、ウォーブルされたプリグルーブでウォーブル処理が施されＡＴＩＰの同期割り込みデータとアドレスデコード結果がＣＰＵ１７に与えられる。

【００２８】再書き込みデータはＨ－ＣＰＵ２６から与

えられ、Ｉ／Ｆ１６及びエンコーダ／デコーダ１５を介してＥＦＭデータはＲＦアンプ９及びレーザ駆動回路８を経てパワーレーザ６を駆動する。

【００２９】更にＣＰＵ１７はＡＤＣ（アナログーデジタル変換器）１８及びＤＡＣ（デジタルーアナログ変換器）１９を有し、ＲＦアンプ９からＡＤＣ１８を介してＲＦ信号をデジタル化したデータがＣＰＵ１７に与えられ、ＣＰＵ１７からＤＡＣ１９を介してセキュリティ情報としての識別データ（ＣＤ－Ｒに透し技術として書き込まれる記録媒体固有の指紋）となるアナログ的なパターン波形が供給される。

【００３０】上述の記録再生装置に於いて、識別データ（以下指紋データと記す）をＣＤ－Ｒ１に書き込む構成を図２及び図３で説明する。図２及び図３で図１との対応部分には同一符号を付して重複説明を省略するが、図２はレーザパワー制御を行う場合であり、図３はフォーカスバイアス制御も行う場合の系統図を示している。

【００３１】図２では、ＣＰＵ１７内に包含されていてもよいが、乱数発生手段２４を用意し、この乱数発生手段２４でランダムデータを発生させる。このランダムデータをＤＡＣ１９に供給して、ＤＡＣ１９でアナログ変換したランダム信号でハイパワーレーザ６のレーザパワーの目標値で振るためにＲＦアンプ９の非反転端子に供給し、反転端子にレーザパワーモニタを接続し、レーザ駆動回路８を介してハイパワーレーザ６を駆動する様にしている。

【００３２】図３では光ピックアップ５のフォーカスバイアス（オフセット）量をランダムデータで振って指紋データを記録層１ｂに書き込むために、ＤＡＣ１９から得たランダム信号を加算アンプ２５の反転端子に供給し、光ピックアップ５とＲＦアンプ９を介して得たＲＦ信号を加算アンプ２５の非反転端子に供給し、加算アンプ出力をサーボ回路２０とフォーカス駆動回路２１ａを介して光ピックアップ５に供給して、フォーカスバイアスを振りながら指紋の書き込みが行われる。

【００３３】上述の図１及び図２で説明した系統図での動作を図４乃至図６のフローチャート及び図７と図８の波形図により説明する。

【００３４】図４はＣＤ－Ｒ１への指紋データの書き込み時のフローチャートを示すものである。図４に於いて、第１ステップS_1 ではＣＤ－Ｒ１の所定位置にアクセスする。

【００３５】第２ステップS_2 では乱数発生手段２４によって、ランダム数値を発生させる。

【００３６】第３ステップS_3 では第２ステップS_2 で得たランダム数値で図２の様にレーザパワーを制御して識別データである指紋データをアナログ的にＣＤ－Ｒ１の所定位置に書き込みを行う。

【００３７】第４ステップS_4 では例えば図７に示す様な所定の再生波形２９の書き込み終了時に書き込みを停止してエンドに至る。

【００３８】図５はＨ－ＣＰＵ２６への指紋データの登録時のフローチャートを示すもので第１ステップST_1 では光ピックアップ５をＣＤ－Ｒ１の所定の指定位置にアクセスする。

【００３９】第２ステップST_2 ではＣＤ－Ｒ１に書き込まれた指紋データの読み出しを開始する。

【００４０】第３ステップST_3 ではＣＤ－Ｒ１に記録された指紋データをＤＡＣ１９を介してデジタルデータに変換してＨ－ＣＰＵ２６に転送する。

【００４１】第３ステップST_3 で例えば指紋データとして図７の如き再生波形２９が得られた場合に時刻t_1，t_2，t_3，t_4 ‥‥t_j ‥‥t_n のＡＤＣ１８によるデジタル変換値を夫々A_1，A_2，A_3，A_4 ‥‥A_j ‥‥A_n とし、データ列全体をＷｖｄｔとし、時刻t_j の時のデジタル変換値A_j でのデータセット値W_j＝（t_j，A_n）とする。

【００４２】上述のデジタル変換値A_j はゲイン等の再生条件や駆動特性のばらつきやＣＤ－Ｒ１の経時変化等で異なってくるので正規化を施す必要が生ずる。

【００４３】例えばｍＴ＝４Ｔの図７に示した繰り返し再生波形２９をＣＤ－Ｒ１に書き込んだ時のピークツウピース（Peak to Peak）のレベルが図８に示す様にV_1，V_2，V_3，V_4 であった時の夫々のＡＤＣ後の値をpk_1，pk_2，pk_3，pk_4 とおくと、このピークツウピース値pk_1 ～pk_4 の平均値ｐｋ・ａｖｅは、

$$pk\cdot ave=(pk_1+pk_2+pk_3+pk_4)/4 \quad \cdots (1)$$

となる。

【００４４】ここでA_j を４Ｔの再生レベルで正規化（Normalize）する。即ち、正規化された波高値をB_j とすれば

$$B_j=A_j/pk\cdot ave \quad \cdots\cdots (2)$$

で表すことが出来る。

【００４５】次に第４ステップST_4 では上述の正規化した再生波形２９をＣＤ－Ｒ１の管理番号と共にＨ－ＣＰＵ２６が有する不揮発性の記憶手段２７に格納し、これをＣＤ－Ｒ１のセキュリティ情報、即ち、指紋データとして登録を終了する。

【００４６】上述の構成ではＣＤ－Ｒ１に記録したランダムなパターン即ち、指紋データをＡＤＣでアナログ波形として取り込み、その波形をＡＤＣを介してＨ－ＣＰＵ２６に格納したが、ＣＤ－Ｒ１のランダムなパターンを通常より速い高速サンプルレートで２値化した指紋データをＨ－ＣＰＵ２６に格納する様にしてもよい。

【００４７】次にＣＤ－Ｒ１への書き込み許可及び不許可処理のフローチャートを図６で説明する。このフローチャートは記録再生装置２８によってＣＤ－Ｒ１に記録

した指紋データを読み出し、Ｈ－ＣＰＵ２６に格納した指紋データと照合を行うもので第１ステップＳＴＰ$_1$ では光ピックアップ５を所定位置にアクセスする。

【００４８】第２ステップＳＴＰ$_2$ ではＣＤ－Ｒ１に書き込んだ指紋データのリードを開始する。

【００４９】Ｈ－ＣＰＵ２６にはＣＤ－Ｒ１のディスク管理番号と共に図７で示した指紋データの全データ列Ｗｖｄｔが登録されているが、これをＷｖｄｔｏとし、上述の（２）式で正規化した波高値Ｂ$_i$ をＲ$_i$ とする。即ち、

Ｒ$_i$ ＝Ｂ$_i$ （１≦ｉ≦Ｓ） ・・・（３）

ここでＳはＷ$_i$ の個数である。

【００５０】第３ステップＳＴＰ$_3$ において、記録再生装置２８は光ピックアップ５を介して読み出したＣＤ－Ｒ１に記録された指紋データをアナログ的に読み出し、ＡＤＣ１８を介してデジタル変換した全データ列ＷｖｄｔをＨ－ＣＰＵ２６側に転送する。

【００５１】第４ステップＳＴＰ$_4$ において、Ｈ－ＣＰＵ２６はＣＤ－Ｒ１のディスク管理番号に対応するディスクの指紋データＷｖｄｔ$_0$ （Ｒ$_i$ の集合）を記憶手段２７から取り出す。

【００５２】第５ステップＳＴＰ$_5$ では第３ステップＳＴＰ$_3$ で転送されて来たＣＤ－Ｒ１の全データ列の指紋データＷｖｄｔ（Ｂ$_i$ の集合）とを比較する。

【００５３】この比較動作は

Ｒ$_i$ ＋Ｗｄｕ＞Ｂ$_i$ ＞Ｒ$_i$ －Ｗｄｌ ・・・（４）

ここで、Ｗｄｕ：上側の許容値 Ｗｄｌ：下側の許容値である。となる。

【００５４】今、Ｆを（４）式を満たすＢ$_i$ （１≦ｉ≦Ｓ）のトータル個数とした時η＝Ｆ／Ｓを定義し、この時、以下の条件を考える。

η＞Ｃ ・・・（５）

ここでＣは許容比率であり例えば７割～９割程度に選択される。

【００５５】第６ステップＳＴＰ$_6$ では（５）式が満足されたか否かを判断する。即ち、比較データが所定の許容比率割合を満たしたかどうかをＨ－ＣＰＵ２６は判断し、（５）式を満たしていなければ第７ステップＳＴＰ$_7$ に進んでＣＤ－Ｒ１への書き込みを禁止する指令を記録再生装置に転送する。

【００５６】一方、第６ステップＳＴＰ$_6$ で（５）式を満足する場合には第８ステップＳＴＰ$_8$ に進んでＣＤ－Ｒ１への書き込み許可指令を記録再生装置に転送する様に成される。

【００５７】本発明は叙上の様に構成し、且つ動作するので偽造不可能な記録媒体及び記録再生装置並びに決済等の重要な電子ファイルを不正に改竄や偽造できない識別方法を簡単な構成で得ることが出来、アナログ的な波形を識別データ（指紋データ）としたので電子認証に対しても強力なプロテクト可能なシステムが得られる。

【００５８】

【発明の効果】本発明の記録媒体によればアナログ的なランダム波形を識別データとして記録しているためデジタル的にセキュリティ情報である識別データを処理する場合に比較して解読し難い識別データによって強力なプロテクトが可能となる。

【００５９】又、本発明の記録媒体の識別方法によれば承認、決済等を必要とする電子ファイルを容易に改竄或は偽造できない識別方法が簡単に得られる。

【００６０】更に、本発明の記録媒体の記録再生装置によれば記録媒体のデータを記録再生可能な光ピックアップを有する記録再生装置であれば、特別の装置を設けずに簡単に識別データを記録可能な記録再生装置が得られる。

【図面の簡単な説明】

【図１】本発明の記録再生装置の系統図である。

【図２】本発明のレーザパワー制御部の系統図である。

【図３】本発明のフォーカスバイアス制御部の系統図である。

【図４】本発明の記録媒体への識別データの書き込みのフローチャートである。

【図５】本発明のホストコンピュータへの識別データの登録時のフローチャートである。

【図６】本発明の記録媒体への書き込み許可、不許可処理のフローチャートである。

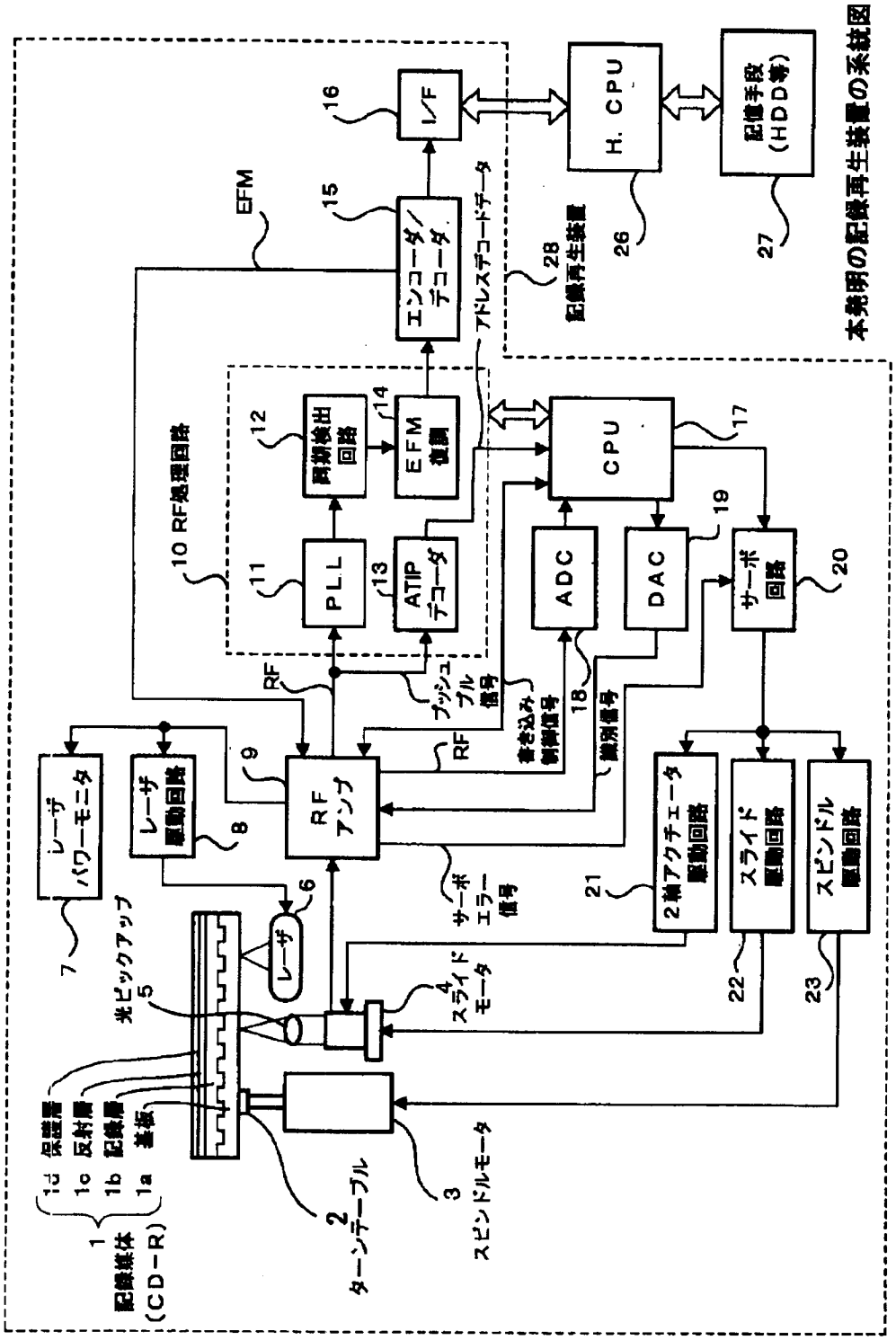
【図７】本発明の動作説明用の再生波形とＡＤＣのサンプルタイミング波形図である。

【図８】本発明の動作説明図のキャリブレーション再生波形図である。

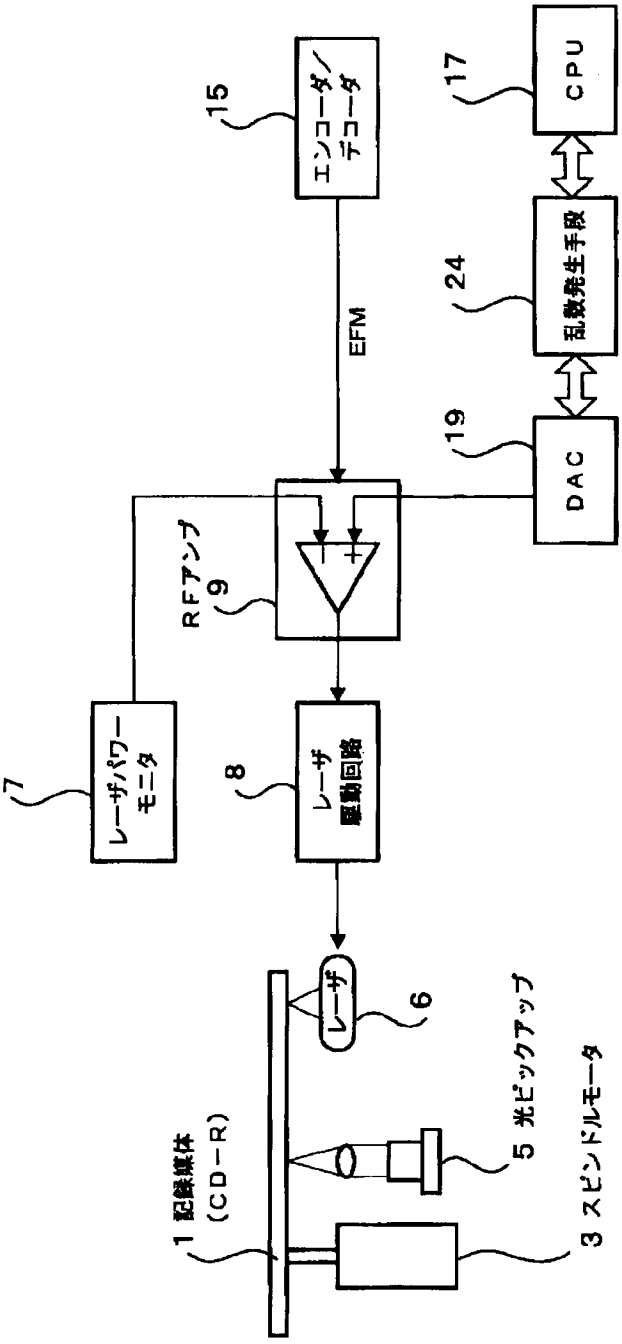
【符号の説明】

１・・・・記録媒体（ＣＤ－Ｒ）、５・・・・光ピックアップ、６・・・・パワーレーザ、８・・・・レーザ駆動回路、９・・・・ＲＦアンプ、１０・・・・ＲＦ処理回路、１７・・・・ＣＰＵ、２４・・・・乱数発生手段、２５・・・・加算アンプ、２６・・・・Ｈ－ＣＰＵ、２７・・・・記憶手段

【図1】

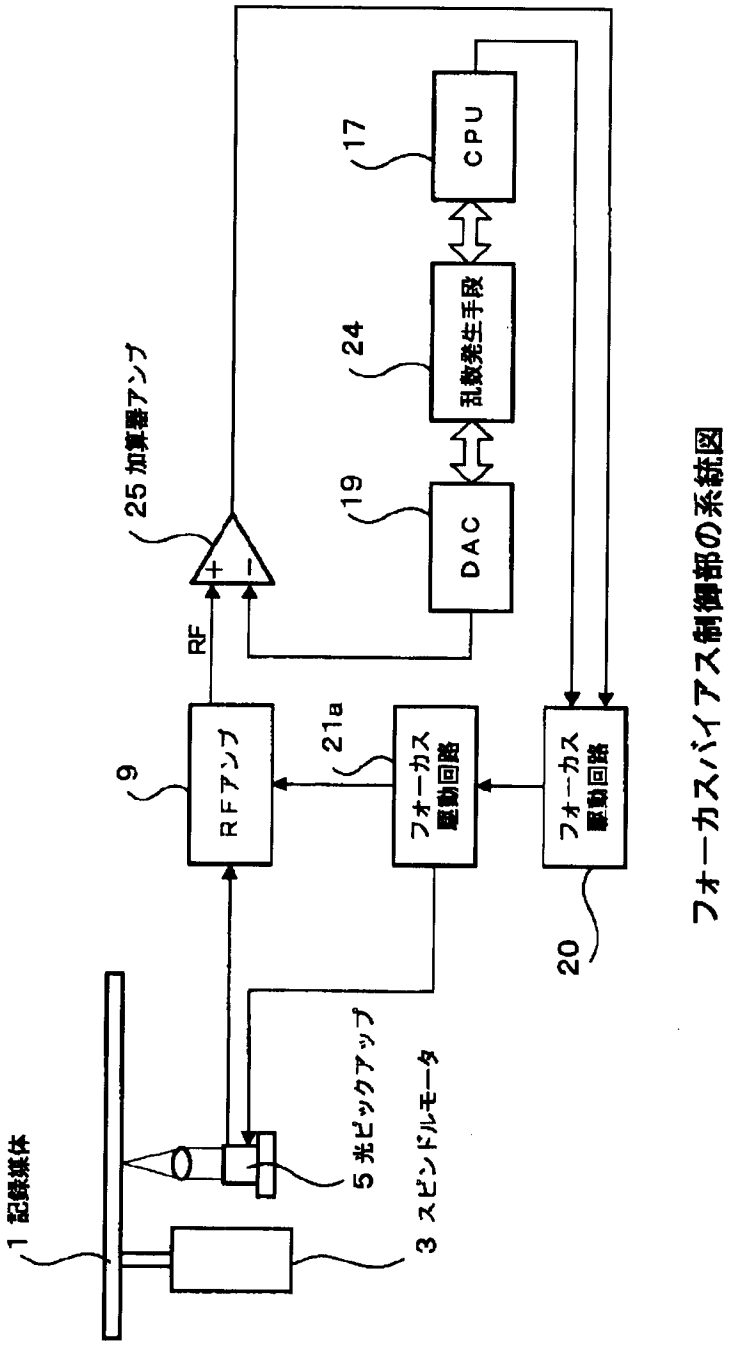

本発明の記録再生装置の系統図
記録再生装置
28
H. CPU
26
記憶手段
(HDD等)
27
I/F
16
エンコーダ/
デコーダ
15
EFM
アドレスデコードデータ
10 RF処理回路
同期検出
回路
12
EFM
復調
14
PLL
11
ATIP
デコーダ
13
CPU
17
ADC
DAC
19
サーボ
回路
20
RF
プッシュプル
信号
書き込み
制御信号
18
識別信号
RF
アンプ
9
レーザ
パワーモニタ
7
レーザ
駆動回路
8
6
レーザ
光ピックアップ
5
サーボ
エラー
信号
21
2軸アクチェータ
駆動回路
スライド
駆動回路
スピンドル
駆動回路
22
23
4
スライド
モータ
3
スピンドルモータ
2
ターンテーブル
1
記録媒体
(CD−R)
1d 保護層
1c 反射層
1b 記録層
1a 基板

【図２】



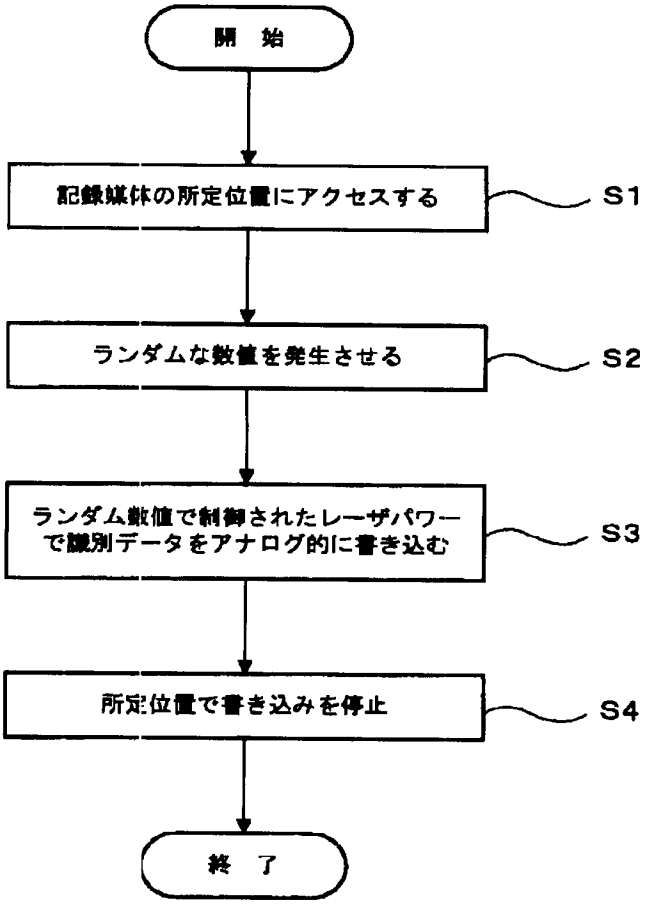
レーザパワー制御部の系統図

【図３】



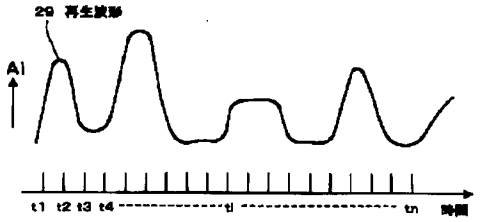
フォーカスバイアス制御部の系統図

【図４】



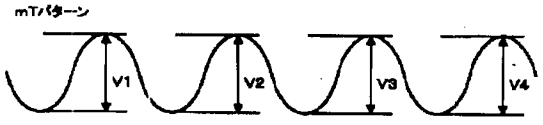
記録媒体への識別データの書き込みのフローチャート

【図７】



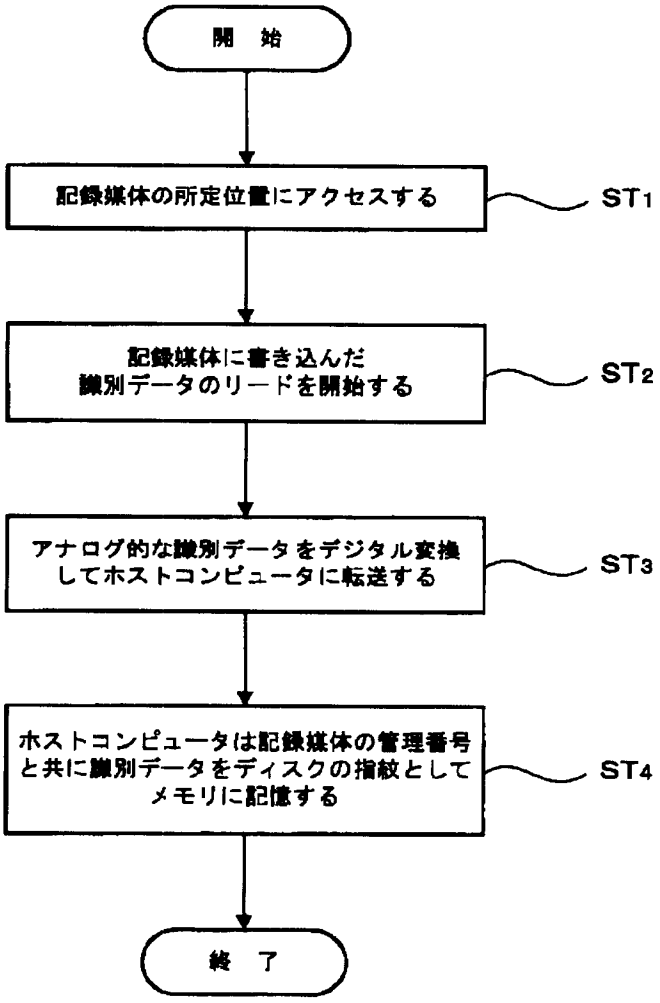
再生波形図とADCのサンプルタイミング波形図

【図８】



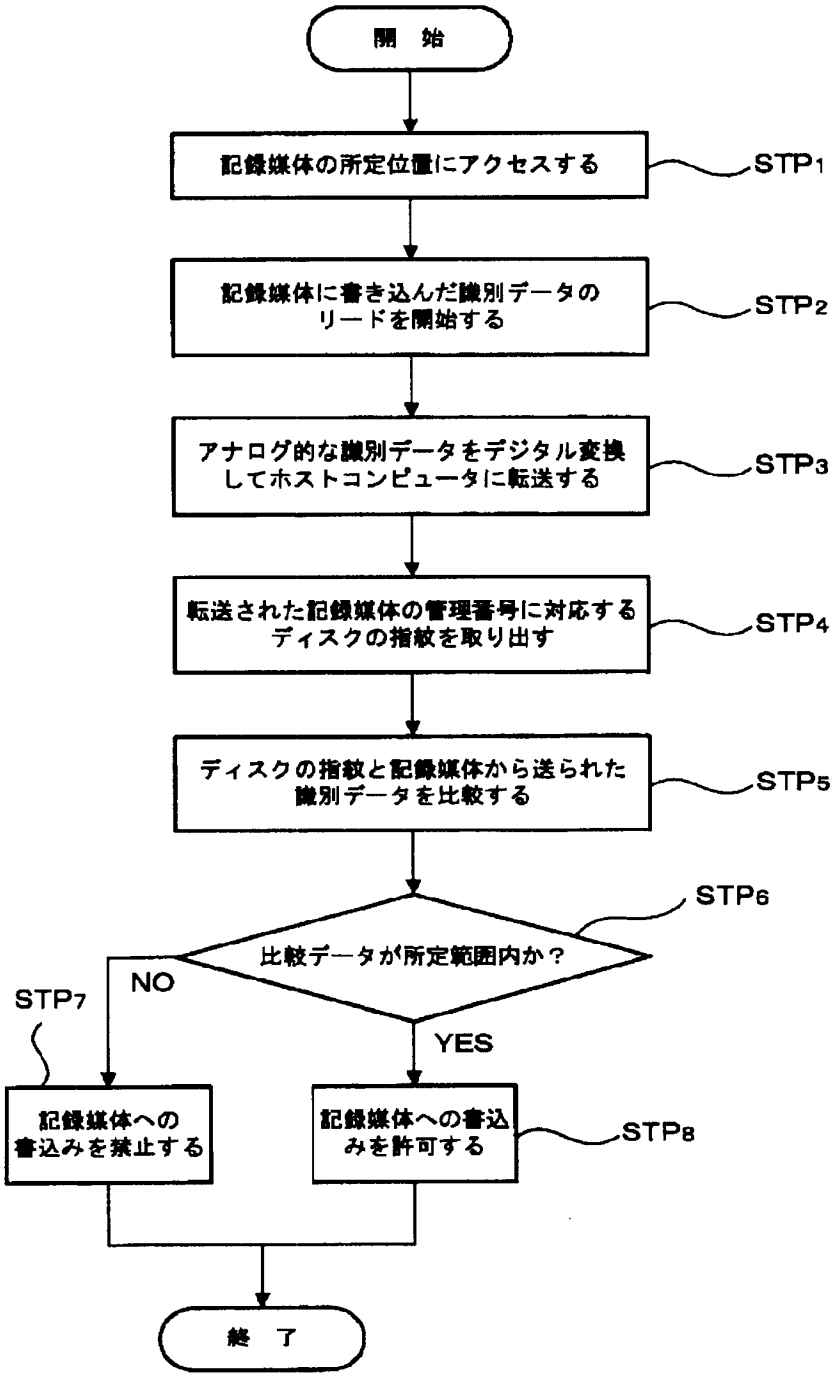
キャリブレーション再生波形図

【図５】



ホストコンピュータへの識別データの
登録時のフローチャート

【図６】



記録媒体への書き込み許可不許可処理のフローチャート